

**IN THE UNITED STATES DISTRICT COURT  
FOR THE NORTHERN DISTRICT OF ILLINOIS  
EASTERN DIVISION**

NATASHA R. JONES, individually and on  
behalf of similarly situated individuals,

Plaintiff,

v.

MICROSOFT CORPORATION,

Defendant.

Case No. 1:22-cv-03437

Hon. Jorge L. Alonso  
Magistrate Hon. Maria Valdez

---

**DEFENDANT MICROSOFT CORPORATION’S REPLY IN SUPPORT OF ITS  
PARTIAL MOTION TO DISMISS**

---

Plaintiff’s Opposition confirms her attempt to stretch BIPA well beyond its plain meaning and the Illinois legislature’s intended reach. Plaintiff alleges that her former employer, Chicago Marriott Suites, and its third-party payroll company, Paychex, Inc., scanned her finger for timekeeping purposes. Because her lawyers already sued Paychex, Plaintiff sued only Microsoft in this case—a company she readily acknowledges she had no relationship with, *see* Opp. at 9—because Paychex used Microsoft’s Azure cloud computing services to store and support its apps and data, allegedly including her biometric data.<sup>1</sup> Plaintiff does not (and cannot) point to any case that has stretched BIPA this far. The Court should reject Plaintiff’s attempt to substantively expand BIPA and should grant Microsoft’s motion to dismiss Plaintiff’s Section 15(b) and 15(d)<sup>2</sup> claims.

---

<sup>1</sup> Plaintiff inexplicably asserts that Paychex is “the second largest customer of Azure.” Opp. at 2. She cites a “customer story” document from Microsoft’s website, but that document contains no such statement.

<sup>2</sup> As Microsoft explained in its Partial Motion to Dismiss, Plaintiff also failed to state a claim under Section 15(c), but since Microsoft filed its Motion, Plaintiff moved to remand her Section 15(a) and (c) claims.

Plaintiff cannot state a claim under Section 15(b) based on Microsoft’s alleged passive possession of biometric data that Plaintiff admits was collected by Paychex and Paychex alone, and then allegedly stored on Azure by Paychex and Paychex alone. Moreover, Plaintiff does not (and cannot) dispute that it would have been practically impossible for Microsoft to obtain prior written consent from her, as Microsoft has no way of knowing or identifying who an Azure customer’s employer-client’s employees are before the Azure customer collects those employees’ biometric data. Indeed, Plaintiff essentially concedes that the only way a company in Microsoft’s position could comply with 15(b) is by contractually requiring its customer to comply with BIPA’s requirements. That is exactly what Microsoft did. Finally, Plaintiff fails to state a claim under Section 15(d) because she pleads only legal conclusions and fails both in the Complaint and in her response to identify any third party to whom Microsoft supposedly disclosed her data.

### **ARGUMENT**

#### **I. Plaintiff Fails to State A Claim Under BIPA Section 15(b).**

##### **A. Microsoft Did Not Take Any “Active Step” to Collect Plaintiff’s Biometric Data, As Required to State A Claim Under Section 15(b).**

Plaintiff argues that Microsoft collected her biometric data because it “stored her and the other putative class members’ biometrics on its own servers,” and that this enabled the Paychex application’s “remote functionality.” Opp. 9.<sup>3</sup> Put differently, Plaintiff alleges that Paychex stored her alleged biometric data on remote Microsoft Azure servers—that is, that Microsoft possessed

---

After meeting and conferring with Plaintiff’s counsel, Microsoft has stipulated that it will not oppose Plaintiff’s Motion to Remand. Dkt. 22. Therefore, Microsoft only addresses the 15(b) and (d) claims here. <sup>3</sup> Plaintiff also argues Microsoft “does not deny that it received and stored Plaintiff’s biometrics.” Opp. at 1. As discussed in Part I (A), Plaintiff cannot state a Section 15(b) claim based only on allegations of providing storage services to a customer who may choose to use those services to store biometrics—more is required. To be clear, however, Microsoft does not concede that Plaintiff’s (or any class member’s) biometric data was ever stored on Azure servers.

her alleged biometric data collected by Paychex. *See* Compl. ¶¶ 21, 24, 32-33. In so asserting, Plaintiff ignores two key points. First, Section 15(b) “doesn’t penalize mere possession of biometric information,” which is all that Plaintiff alleges here. *King v. PeopleNet Corp.*, 2021 WL 5006692, at \*8 (N.D. Ill. Oct. 28, 2021); *see Namuwonge v. Kronos, Inc.*, 418 F. Supp. 3d 279, 282, 286 (N.D. Ill. 2019) (finding plaintiff’s allegation that her employer stored her fingerprint data in its defendant-supplied database insufficient to state a Section 15(b) claim against the defendant). Second, Section 15(b) does not apply to storage of data after its collection.<sup>4</sup> *See Vance v. Microsoft Corp.*, No. C20-1082JLR, 2022 WL 9983979, at \*7 (W.D. Wash. Oct. 17, 2022) (Section 15(b) “regulates only the acquisition of data, rather than the encrypted storage of data after it is acquired”). Rather, a Section 15(b) claim requires Plaintiff to plausibly allege that Microsoft *itself* collected or obtained Plaintiff’s biometric data. To do so, Plaintiff must allege that Microsoft took an “active step” to collect the data, which Plaintiff does not and cannot allege.

In her Opposition, Plaintiff claims that: (1) cases holding that Section 15(b) requires allegations of an active step are wrongly decided; and (2) Microsoft took an active step because it “actively entered into business with Paychex ... knowing that their partnership would involve collection and storage of copious amounts of employees’ biometrics.” Opp. 7. Both arguments lack any merit.

**1. Section 15(b) Does Not Apply Where the Defendant Did Not Take an Active Step to Collect Biometrics from Plaintiff.**

Plaintiff does not dispute that Section *15(a)*, not Section *15(b)*, requires companies to develop and comply with a retention schedule if they are “*in possession of* biometric identifiers or biometric information.” (Emphasis added.) Nor does she dispute that Section 15(b) doesn’t use the

---

<sup>4</sup> As discussed below, Section 15(a), which is not the subject of Microsoft’s motion to dismiss, regulates possession and storage of biometric data. Yet Plaintiff continually combines the terms “collection” and “storage” even though these are distinct concepts under BIPA.

word “possession” but instead provides that a private entity “may not collect, capture, purchase, receive through trade, or otherwise obtain” biometric data without first obtaining informed written consent from the data subject. 740 ILCS 14/15(a), (b). Thus, these two subsections use different words (“possession” versus “collect, capture, purchase, receive through trade, or otherwise obtain”), and distinct phrasing (the passive “*in possession of*” versus the active “may not collect, capture, receive through trade, or otherwise obtain”). Such distinctions in statutory language matter and must be given meaning under Illinois principles of statutory interpretation. *See Roselle Police Pension Bd. v. Vill. of Roselle*, 905 N.E.2d 831, 834 (Ill. 2009) (under Illinois law, “statute[s] should be evaluated as a whole, with each provision construed in connection with every other section”); *Stauffer v. Innovative Heights Fairview Heights, LLC*, 2022 WL 3139507, at \*4 (S.D. Ill. Aug. 5, 2022) (explaining that courts in the Seventh Circuit have interpreted Section 15(b) to require an active step “[t]o recognize and honor this ***intentional distinction*** in the language used by the Illinois legislature in different sections of BIPA”) (emphasis added).

Not surprisingly, then, courts in the Seventh Circuit consistently recognize and honor this statutory language by holding that “for Section 15(b)’s requirements to apply, an entity must, at a minimum, take an active step to collect, capture, purchase, or otherwise obtain biometric data.” *Jacobs v. Hanwha Techwin Am., Inc.*, No. 21 C 866, 2021 WL 3172967, at \*2 (N.D. Ill. July 27, 2021); *see also Patterson v. Respondus, Inc.*, No. 20 C 7692, 2022 WL 860946, at \*25 (N.D. Ill. Mar. 23, 2022) (same); *Heard v. Becton, Dickinson & Co. (“Heard I”)*, 440 F. Supp. 3d 960, 966 (N.D. Ill. 2020) (same). Plaintiff does not meaningfully address these cases—she does not even

cite *Jacobs* or *Patterson*—and these cases make clear that a defendant does not violate Section 15(b) by merely possessing biometric data.

The cases clarify that an “active step” is some direct action by the defendant to collect biometric data from the plaintiff, generally through the control and use of biometric scanning technology. *See, e.g., Smith v. Signature Sys., Inc.*, 2021-CV-02025, 2022 WL 595707, at \*4 (N.D. Ill. Feb. 28, 2022) (plaintiff adequately alleged an active step where she alleged that defendant, “through its [biometric scan technology], ‘scan[s] and collect[s] ... digital copies of [its client’s employees’] fingerprints”); *Ronquillo v. Doctor's Associates, LLC*, 21 C 4903, 2022 WL 1016600, at \*3 (N.D. Ill. Apr. 4, 2022) (plaintiff adequately alleged an active step where he alleged that defendant “uses [biometric scan technology], which [defendant] exclusively controls, to capture workers’ fingerprints and create the reference templates”). It follows that a defendant does *not* take an active step to collect biometric data from a plaintiff if it does not take any action at all to collect it from her, much less a direct action. *See, e.g., Namuwonge v. Kronos, Inc.*, 418 F. Supp. 3d 279, 286 (N.D. Ill. 2019) (plaintiff failed to state a claim under Section 15(b) where she alleged that her employer “collected the fingerprints using a system that [the defendant] supplied to [the employer]”); *Jacobs*, 2021 WL 3172967, at \*3 (plaintiff failed to allege an active step where “a complete reading of the complaint makes clear that defendant is merely a third-party technology provider (that is, merely provided the cameras), and that the active collector and processor of the data is [defendant’s retail store customer]”).

Attempting to circumvent the plain language application of these cases, Plaintiff cites a recent outlier ruling on a motion in limine in which Judge Kennelly supposedly declined to follow the “active step” case law. *See* Opp. 2, 6–8 (citing *Rogers v. BNSF Ry. Co.*, No. 19-cv-03083, 2022 WL 4465737, at \*3 (N.D. Ill. Sept. 26, 2022)). Plaintiff claims this decision means that “an

‘active step’ requirement is ‘a dubious proposition’ because ‘it amounts to adding language that the statute doesn’t include.’” Opp. 6. But quite the opposite, courts holding Section 15(b) requires an active step of collection by the defendant are interpreting the statute as written, giving force to the distinction between Section 15(b)’s “collect” language and Section 15(a)’s mere “possession” language. In doing so, these courts are properly interpreting the statute as a whole, as Illinois law requires. *See Stauffer*, 2022 WL 3139507, at \*4 (collecting cases).

Indeed, during a later hearing in *Rogers*, Judge Kennelly also recognized the statutory distinction between possession and collection. No. 19-cv-03083, Trial Tr. 1269:13–19 (N.D. Ill. Oct. 11, 2022) (stating “there’s nothing in [Section 15(b)] that says possession is good enough” to support liability; “[t]here’s nothing in here that so much as hints at that ... You have to have done something”), attached as **Exhibit A**. In addition, Microsoft stands in a very different relationship to Plaintiff’s data than the defendant in *Rogers*. There, the defendant allegedly contracted with a vendor to collect biometric data on the defendant’s behalf. *Rogers*, 2022 WL 4465737, at \*3. Plaintiff does not and cannot allege that Microsoft contracted with anyone to collect her biometric data on Microsoft’s behalf.

Plaintiff also claims that “[o]ther courts in this District have reached the same conclusion [as Judge Kennelly].” Opp. 6 (citing *Figueroa v. Kronos, Inc.*, 454 F. Supp. 3d 772, 783-84 (N.D. Ill. 2020); *Heard v. Beckton, Dickinson & Co.*, 524 F. Supp. 3d 831, 841 (N.D. Ill. 2021) (“*Heard II*”). Neither *Figueroa* nor *Heard II* supports Plaintiff’s argument. In *Figueroa*, the defendant supplied biometric timekeeping equipment directly to the plaintiffs’ employer and the plaintiffs alleged that their employer “scan[ned] their fingerprints using [defendant’s] device” and “that [defendant] ‘stored,’ ‘used,’ and ‘disclosed’ Plaintiffs’ biometric data.” *Figueroa*, 454 F. Supp. 3d at 779, 784. Here, in contrast and as Microsoft showed in its Motion, Plaintiff admits it was

Paychex who her employer Marriott used to collect biometric data, and it was Paychex, using Paychex's own Paychex Flex Time software, who collected her alleged biometrics—not Microsoft. *See* Compl. ¶¶ 27, 29, 39; Mot. at 7-8.

And in *Heard II*, the court denied defendant's motion to dismiss the amended complaint *without* disturbing its ruling on an earlier motion to dismiss, which dismissed plaintiff's Section 15(b) claim because he "ha[d] not adequately pleaded that [the defendant] took [an active step under Section 15(b)]." *Heard I*, 440 F. Supp. 3d at 966. What's more, the *Heard II* court, far from rejecting the "active step" analysis as Plaintiff argues, reaffirmed it and found plaintiff's amended complaint "has sufficiently *alleged an active step* by [the defendant] to collect, capture, or otherwise obtain [plaintiffs'] biometric data" because Plaintiff alleged "the [defendant's] device scans the user's fingerprint, extracts the unique features of that fingerprint to create a user template, and then stores users' biometric information both on the device *and* in [the defendant's] servers." *Heard II*, 524 F. Supp. 3d at 841 (emphasis added). There are no such allegations of active collection by Microsoft in this case.

Finally, Plaintiff argues that "[r]eading an 'active step' requirement into Section 15(b) would render the phrase 'otherwise obtain' superfluous" because, she says, "otherwise obtain" is a "'rather broad' term meant to serve as a 'catch-all phrase.'" <sup>5</sup> Opp. 7. Even so, under "the cardinal rule of [Illinois] statutory construction known as *ejusdem generis*," the term "otherwise obtain" must be interpreted to mean "other such like" the preceding terms. *Pooh-Bah Enterprises, Inc. v. Cnty. of Cook*, 232 Ill. 2d 463, 492, 905 N.E.2d 781, 799 (Ill. 2009). This means "otherwise

---

<sup>5</sup> Plaintiff quotes this language from *Vance v. Amazon.com Inc.*, 525 F. Supp. 3d 1301, 1312 (W.D. Wash. 2021). On October 17, 2022, the court granted summary judgment in favor of Amazon on all the plaintiffs' BIPA claims. *Vance v. Amazon.com, Inc.*, 2022 WL 12306231 (W.D. Wash. Oct. 17, 2022). On the same day, the court granted summary judgment for Microsoft on the same plaintiffs' BIPA claims, which plaintiffs had asserted on the same legal theory. *Vance*, 2022 WL 9983979.

obtain” in Section 15(b) is confined by the preceding terms “collect, capture, purchase, [and] receive through trade.” 740 ILCS 14/15(b). Each of these words involve action. As Judge Kennelly explained, for Section 15(b) to apply, “possession is not enough ... You have to have done something.” Ex. A, Trial Tr. 1269:13–19. Plaintiff cites no case holding a court may ignore this settled principle of statutory interpretation. The Court should decline Plaintiff’s invitation to depart from the plentiful case law properly interpreting Section 15(b) under Illinois law to require an “active step” by the defendant to collect the plaintiff’s biometric data.

**2. Contracting with Paychex Does Not Constitute an Active Step Under Section 15(b) Claim.**

Attempting to save her Section 15(b) claim, Plaintiff argues Microsoft nevertheless took an active step to collect her biometric data because it “actively entered into business with Paychex ... knowing that their partnership would involve collection and storage of copious amounts of employees’ biometrics.” Opp. 7. But even if that were true (which Microsoft does not concede) “actively entering into business” with a third-party is not the type of action covered by Section 15(b), which instead focuses on the point of collection of a person’s biometric data. To hold otherwise would mean any company doing business with or licensing technology to another company that uses biometrics for its own purposes would suddenly be subject to liability under BIPA.

Instead, case law makes clear that the “active step” required under Section 15(b) must be a step taken by the defendant in the actual collection of biometric data from the plaintiff—here, the scanning of Plaintiff’s fingerprints. Plaintiff readily admits it was *Paychex* who did that—not Microsoft. Compl. ¶¶ 27, 29. And she does not allege Microsoft engaged Paychex to collect Plaintiff’s biometrics *for Microsoft’s* own purposes. Nor could she so allege, as Microsoft’s role was to provide data computing and storage services via its Azure datacenters to Paychex for



Paychex to use however it chose. *See* Compl. ¶¶ 23, 25-28, 41. Paychex, not Microsoft, was responsible for complying with laws that apply to the data Paychex collects. *See* Mot. at 10 n. 5 (citing Microsoft’s publicly available Products and Services Data Protection Addendum, which provides that “Microsoft does not determine whether Customer’s data includes information subject to any specific law or regulation . . . Customer must comply with all laws and regulations applicable to its use of Products and Services, including laws related to biometric data.”)

Plaintiff may not state a claim *against Microsoft* under Section 15(b) by merely repeating that Microsoft entered into a business agreement with Paychex for general cloud storage and computing services, given Paychex and Paychex alone collected the alleged biometric data for its *own* clients using Paychex’s *own* technology. *See* Mot. at 7-8; Compl. ¶¶ 27-30.

Ignoring the distinction between “possession” and “collection,” Plaintiff claims Microsoft “necessarily had to actively obtain [her biometric] information first” to store it. Opp. 8. Accepting Plaintiff’s theory would not only disregard the plain words of the statute but would also mean that any entity who “possesses” biometric data under Section 15(a) necessarily also “collected” or “obtained” that data from the plaintiff under Section 15(b). But there is no question that one can “possess” something without first actively “collecting” or “obtaining” it, which is the precise distinction the “active step” cases recognize. *See, e.g., Jacobs*, 2021 WL 3172967, at \*2 (“Section 15(b) requires something more than mere possession”); *King*, 2021 WL 5006692, at \*8 (same); *Namuwonge*, 418 F. Supp. 3d at 282-284, 286 (plaintiff sufficiently pleaded possession but not collection where she alleged her data was stored in defendant’s database but that only her employer

“collected employee's fingerprints using a system that [the defendant] supplied”). Plaintiff's argument lacks support in the statute and case law, and the Court should reject it.

Because Plaintiff does not (and cannot) allege facts plausibly showing Microsoft itself took an active step to collect, capture, purchase, receive through trade, or otherwise obtain her biometric data, the Court should dismiss her claim under Section 15(b) with prejudice.

**B. Section 15(b) Does Not Apply Where a Private Entity Has No Practical Way to Identify Plaintiffs and Obtain Consent.**

Microsoft showed that Section 15(b) does not apply where, as here, a cloud service provider has no feasible means of identifying and contacting those whose biometric information *others* have collected and stored in the cloud, much less of doing so before that collection and storage occurs. Mot. 9. This is so because, as Microsoft explained, it has no practical way to identify Plaintiff and provide notice to and obtain consent from her *before* Paychex conducts its collection, as Microsoft is a cloud services provider *twice*-removed from Plaintiff. In response, Plaintiff mischaracterizes *Zellmer v. Facebook*, No. 3:18-CV-01880-JD, 2022 WL 976981 (N.D. Cal. Mar. 31, 2022). But there, the court not only emphasized that the plaintiffs were “total strangers” to the defendant, but also that the defendant had no realistic way to provide notice to and obtain consent from unknown non-users. *Id.* at \*4–5. Plaintiff does not meaningfully respond to this latter point.

Instead, she cites four distinguishable cases in which the plaintiffs alleged the defendant *did have* practical ways to identify plaintiffs and secure prior consent, assuming it was required. *Figueroa*, 454 F. Supp. 3d at 783 (holding that Section 15(b) applied where defendant had the ability to identify employees because the defendant provided biometric timekeeping equipment and directly collected the employees' biometric data); *Flores v. Motorola Sols., Inc.*, No. 1:20-CV-01128, 2021 WL 232627, at \*1 (N.D. Ill. Jan. 8, 2021) (denying motion to dismiss where the

defendants “maintain[ed] a gallery of over 18 million public booking photographs (or ‘mugshots’)” which they sold to law enforcement agencies for the purpose of identifying suspects); *Monroy v. Shutterfly, Inc.*, No. 16 C 10984, 2017 WL 4099846, at \*1 (N.D. Ill. Sept. 15, 2017) (holding that Section 15(b) applied where defendant Shutterfly prompted users to identify unknown facial images by name); *Wise v. Ring LLC*, No. C20-1298-JCC, 2022 WL 3083068, at \*3 (W.D. Wash. Aug. 3, 2022) (holding that Section 15(b) applied and distinguishing *Zellmer* because the plaintiff alleged that the defendant’s “patent applications describe a system capable of immediately identifying individuals” based on facial recognition and that defendant “partners with law enforcement agencies to semi-automatically identify individuals based on face recognition”).

Here, Plaintiff does not and cannot plausibly allege that Microsoft conducted any biometric scanning of her fingers or supplied any biometric scanning equipment to Paychex. Quite the opposite, Plaintiff repeatedly admits that it was Paychex who collected her biometrics using Paychex’s Flex Time program. Compl. ¶¶ 27, 29. And Plaintiff does not allege how Microsoft could determine the identity of all or any of Paychex’s employer-customers, let alone identify which of Paychex’s employer-customers had engaged Paychex to collect biometric data from their employees and if so, from which employees—and all before the point of collection. This is so because Plaintiff does not and cannot allege Microsoft had any information about Plaintiff, such as information about her identity or access to a law enforcement database—unlike the defendants in *Flores*, *Monroy*, and *Wise*. In this way, Microsoft is in exactly the same situation as the defendant in *Zellmer*—unable to identify the individuals from whom Paychex collected alleged biometric data. Applying Section 15(b) to Microsoft here would mean Microsoft “in effect would need to identify every non-user [here, Microsoft’s customers’ employer-customers’ employees] in Illinois on a regular basis, and figure out a way to communicate with them to provide notice and

obtain consent.” *Zellmer*, 2022 WL 976981, at \*4. That is not what Section 15(b) requires or was intended to require.

Plaintiff cites *Figueroa* to suggest Microsoft could comply with Section 15(b) by requiring the entity with the realistic ability to provide notice to and obtain consent from data subjects (here, Paychex) to comply with BIPA through contractual preconditions. Opp. 10. But that is exactly what Microsoft did, as Plaintiff admits in her Opposition. Opp. 10. Microsoft’s contract with Paychex required Paychex to “comply with all laws and regulations applicable to its use of [Microsoft’s] Products and Services, including laws related to biometric data....” Mot. Ex. C, Dkt. 16-3 at 5. As Microsoft explained in its Motion, the DPA also requires Azure customers to ‘provid[e] notice to’ and ‘obtain[] consent from’ individuals before collecting their biometric data, when required by law. Mot. 12 n.6. Plaintiff argues Paychex failed to comply with these contractual provisions (and her counsel has already sued Paychex on that basis). Paychex’s non-compliance does not somehow make Section 15(b) applicable to Microsoft, and Plaintiff cites no authority holding otherwise. On the contrary, Plaintiff’s own admission shows Microsoft did all it could to ensure its customers would comply with Section 15(b)—*i.e.*, Microsoft required its customer, the entity in a position to provide prior notice to and obtain consent from Plaintiff, to comply with BIPA as a contractual condition to using Microsoft’s services.

As the Illinois Supreme Court has stated, “compliance” with BIPA “should not be difficult.” *Rosenbach v. Six Flags Entertainment*, 129 N.E.3d 1197, 1207 (Ill. 2019). Illinois courts “presume[] that the legislature did not intend absurd, inconvenient, or unjust results.” *Sigcho-Lopez v. Illinois State Bd. of Elections* --- N.E.3d ---, 2022 WL 869783, at \*5 (Ill. 2022). Plaintiff’s proposed interpretation of BIPA, however, would force Microsoft into an impossible task of somehow having to identify more than 80,000 employees (according to Plaintiff) of its

customers' employer-clients, and to do so *before* its customers collected biometric data from the employees of those customers' employer-clients. Otherwise, and absurdly, Microsoft would have already violated BIPA by the time it allegedly came into possession of the biometric data. But construing BIPA this way "would lead to obvious and insoluble problems." *Zellmer*, 2022 WL 976981, at \*4. The Court should not accept Plaintiff's untenable theory and should dismiss the Section 15(b) claim on this additional basis.

## **II. The Court Should Dismiss Plaintiff's Section 15(d) Claim Because She Does Not Plausibly Allege "Disclosure," "Redisclosure," or "Dissemination."**

Plaintiff does not dispute that allegations that do no more than parrot Section 15(d)'s language, without details such as when or to whom a defendant disclosed biometric data, do not suffice on a motion to dismiss. Mot. at 15; *Carpenter v. McDonald's Corp.*, 2022 WL 897149, at \*4 (N.D. Ill. Jan. 13, 2022); *see also Horn v. Method Prod., PBC*, No. 21 C 5621, 2022 WL 1090887, at \*3 (N.D. Ill. Apr. 12, 2022) (dismissing Section 15(d) claim where the complaint "[did] not contain any specifics concerning the basis for [the plaintiff's] belief that [the defendant] disclosed his biometric information"). But bare conclusions of law are all Plaintiff has pleaded. In her Opposition, Plaintiff points to the single allegation that "after Plaintiff's ... biometric identifiers were obtained by Defendant through its clients' platforms, Defendant disclosed or otherwise disseminated their biometrics" without consent. *See* Opp. 14 (citing Compl. ¶¶ 90–91)). But on its face this allegation fails to identify when or to whom Microsoft alleged made this dissemination or disclosure.

To sidestep the inadequacy of this pleading, Plaintiff asks the Court to allow her to proceed with discovery on her Section 15(d) claim. Opp. 15. In so arguing she relies on *Heard II*, where the plaintiff alleged the defendant disclosed his data to "currently unknown" third parties "that host biometric data in their data center(s)." *Id.* (citing *Heard II*, 524 F. Supp. 3d at 837). But

Plaintiff pleads no similar facts here, which the *Heard II* court already recognized as “quite thin.” *Heard II*, 524 F. Supp. 3d at 843.

Plaintiff may not “unlock the doors of discovery” based on “nothing more than conclusions.” *Ashcroft v. Iqbal*, 556 U.S. 662, 678–79 (2009); *see also Martin v. CareerBuilder, LLC*, No. 19-cv-6463, 2020 WL 3578022, at \*5 (N.D. Ill. July 1, 2020) (“Plaintiff argues that . . . they should get a crack at discovery before the Court dismisses this complaint. This argument has it backwards. The Court must dismiss speculative suits ‘lest a plaintiff with a largely groundless claim be allowed to take up the time of a number of other people, with the right to do so representing an *in terrorem* increment of the settlement value.’”) (quoting *Bell Atl. Corp. v. Twombly*, 550 U.S. 544, 558 (2007)). Plaintiff asks this Court to permit discovery based on two sentences in Count IV of her Complaint that merely restate BIPA’s statutory language. She does not identify anyone to whom Microsoft supposedly disclosed her alleged biometric data; she does not even allege that such an entity might exist but is currently unknown. These allegations are insufficient under federal pleading standards, and this Court should dismiss Plaintiff’s claim with prejudice.

### **CONCLUSION**

The Court should dismiss Plaintiff’s claims under BIPA Sections 15(b) and (d) with prejudice.

DATE: October 28, 2022

**MORGAN, LEWIS & BOCKIUS LLP**

*/s/ Elizabeth B. Herrington*

---

Elizabeth B. Herrington

Gregory T. Fouts

Benjamin Kabe

110 North Wacker Drive, Suite 2800

Chicago, Illinois 60606

T: (312) 324-1445

F: (312) 324-1001

beth.herrington@morganlewis.com

gregory.fouts@morganlewis.com

benjamin.kabe@morganlewis.com

*Counsel for Defendant Microsoft Corporation*

**CERTIFICATE OF SERVICE**

I hereby certify that on this 28th day of October, 2022, I caused a true and correct copy of the foregoing **Reply in Support of Partial Motion to Dismiss** to be filed through the Court's CM/ECF System and served the below Counsel of Record via electronic mail:

Myles McGuire  
Paul T. Geske  
Steven R. Beckham  
MCGUIRE LAW, P.C.  
55 W. Wacker Drive, 9th Fl.  
Chicago, IL 60601  
Tel: (312) 893-7002  
Fax: (312) 275-7895  
mmcguire@mcgpc.com  
pgeske@mcgpc.com  
sbeckham@mcgpc.com

/s/ Elizabeth B. Herrington  
Elizabeth B. Herrington